UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/578,868	05/11/2006	Masaki Hamada	288056US40PCT	3257

22850   7590   10/22/2008
OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER
CHAI, LONGBIT

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
10/22/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>14 May 2007</u>.
2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>16-28</u> is/are pending in the application.
     4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) <u>16-28</u> is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.
10) ☒ The drawing(s) filed on <u>11 May 2006</u> is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
     a) ☒ All   b) ☐ Some * c) ☐ None of:
       1. ☒ Certified copies of the priority documents have been received.
       2. ☐ Certified copies of the priority documents have been received in Application No. _____.
       3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
     * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
     Paper No(s)/Mail Date <u>5/14/2007</u>.

4) ☐ Interview Summary (PTO-413)
     Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Priority

1.   Applicant's claim for benefit of foreign priority under 35 U.S.C. 119 (a) – (d) is

acknowledged.

The application is a 371 case of PCT/JP05/15156 application filed on 8/19/2005 and has

a foreign priority application filed on 10/28/2004.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

2.   Claims 16 – 19, 21, 22, 24 – 26 and 28 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Kanno et al. (U.S. Patent 2004/0064738), in view of Bang et al. (Korea KR-

10-2004-0036228).

As per claim 16 and 28, Kanno teaches an denial-of-service attack detecting system for

detecting a denial-of-service attack on a communication device (Kanno: Abstract), the denial-of-

service attack detecting system comprising:

a performance measuring device that measures performance of the communication

device (Kanno: Figure 9 / Element 908 and Para [0143] Line 7 – 9: a processing situation

reception unit measures the performance (traffic load) of the server);

Kannon does not disclose expressly a monitoring device that monitors a packet transmitted to a communication device that is a target of the denial-of-service attack.

Bang teaches a monitoring device that monitors a packet transmitted to a communication device that is a target of the denial-of-service attack (Bang: Abstract: a traffic monitoring unit periodically monitors traffic change against a pre-set reference value and detects an IP packet having the traffic component exceeding the pre-set reference value).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Bang within the system of Kannon because (a) Kannon teaches detecting a denial of service attack on the server based upon the performance level of load state of the data request / response traffic (Kannon: Abstract), and (b) Bang teaches providing a traffic monitoring unit for detecting a denial of service attack on the packet level by periodically monitors traffic change against a pre-set reference value by detecting an IP packet having the traffic component exceeding the pre-set reference value (Bang: Abstract).

an attack determining device that performs communication with the monitoring device and the performance measuring device (Kanno: Figure 1 / Element 103, Figure 2 & 9 and Para [0044]: server computer protection apparatus communicates with the monitoring device and the performance measuring device to determine the DoS attacks) , wherein

the monitoring device includes a traffic abnormality detecting unit that detects traffic abnormality information indicating an abnormality of traffic due to the packet with respect to the communication device (Bang: Abstract: a traffic monitoring unit periodically monitors traffic change against a pre-set reference value and detects an IP packet having the traffic component exceeding the pre-set reference value),

the performance measuring device includes a performance abnormality detecting unit that detects performance abnormality information indicating an abnormality of throughput of the

communication device (Kanno: Para [0143] Line 7 – 9, Para [0044] and [0152]: a processing

situation reception unit measures the performance (traffic load) of the server), and

the attack determining device includes an effects determining unit that determines

whether the communication device received the denial-of-service attack, based on the traffic

abnormality information and the performance abnormality information (Kanno: Figure 1 /

Element 103, Figure 2 & 9 and Para [0044]: server computer protection apparatus determines

the situations of DoS attack).

As per claim 17, Kanno as modified teaches the monitoring device further includes a

traffic-abnormality-information transmitting unit that transmits the traffic abnormality information

to the attack determining device (Bang: Abstract: the monitoring device transmitting the event to

the security management device).

As per claim 18, Kanno as modified teaches the performance measuring device further

includes a performance-abnormality-information transmitting unit that transmits the performance

abnormality information to the attack determining device (Kannon: Figure 9 and Para [0152]: the

transmitting unit of the processing situation reception unit transmits the performance

abnormality information to the server computer protection apparatus for decision making on

DoS attack).

As per claim 19, Kanno as modified teaches the traffic abnormality detecting unit detects

the traffic abnormality information based on a predetermined attack detection condition that is

set in advance (Bang: Abstract: a traffic monitoring unit periodically monitors traffic change

against a pre-set reference value and detects an IP packet having the traffic component

exceeding the pre-set reference value).

As per claim 21, Kanno as modified teaches the traffic abnormality detecting unit detects

the traffic abnormality information based on a steady traffic indicating an average traffic of the

packet transmitted to the communication device (Bang: Abstract).

As per claim 22, Kanno as modified teaches the performance abnormality detecting unit

detects the performance abnormality information based on a predetermined performance

abnormality detection condition that is set in advance (Kanno: Para [0044]).

As per claim 24, Kanno as modified teaches the performance abnormality detecting unit

detects the performance abnormality information based on a steady performance indicating an

average performance feature of the communication device (Kanno: Para [0143] Line 7 – 9: a

processing situation reception unit measures the performance (traffic load) of the server is on an

average level of traffic load).

As per claim 25, Kanno as modified teaches the effects determining unit determines that

the communication device received the denial-of-service attack, when it is determined that one

of the traffic abnormality information and the performance abnormality information causes an

occurrence of other of the traffic abnormality information and the performance abnormality

information based on an abnormality occurrence time included in the traffic abnormality

information and the performance abnormality information (Kanno: Para [0044] and [0036]).

As per claim 26, Kanno as modified teaches when the effects determining unit determines that the communication device received the denial-of-service attack, the attack determining device transmits the traffic abnormality information and the performance abnormality information used for the determination to a device for reporting to an operator (Bang: Abstract: the monitoring device transmitting the event to the security management device).

3.   Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kanno et al. (U.S. Patent 2004/0064738), in view of Bang et al. (Korea KR-10-2004-0036228), and in view of Ioele et al. (U.S. Patent 7,007,299).

As per claim 20, Kanno as modified does not disclose expressly a signature generating unit that generates a signature indicating a feature of the packet attacking the communication device, based on the attack detection condition, and the traffic abnormality information includes the signature.

Ioele teaches a signature generating unit that generates a signature indicating a feature of the packet attacking the communication device, based on the attack detection condition, and the traffic abnormality information includes the signature (Ioele: Column 6 Line 34 – 41 / Line 49 – 55: the intrusion detectors monitor network traffic for attack signatures and alert a security manager when an attack is detected).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Ioele within the system of Kannon as modified because (a) Kannon teaches detecting a denial of service attack on the server based upon the performance level of load state of the data request / response traffic (Kannon: Abstract), and (b)

Ioele teaches providing a traffic monitoring unit for detecting a denial of service attack by

running on a dedicated host and monitor network traffic for attack signatures and alert a security

manager when an attack is detected (Ioele: Column 6 Line 34 – 41 / Line 49 – 55).

4.   Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kanno et al.

(U.S. Patent 2004/0064738), in view of Bang et al. (Korea KR-10-2004-0036228), and in view of

Patrick et al. (U.S. Patent 7,310,684).

        As per claim 23, Kanno as modified does not disclose expressly the performance

abnormality detection condition includes a response time from transmission of a response

request message to the communication device to reception of a response message

corresponding to the response request message, and number of times that the response time

exceeds a predetermined threshold.

        Patrick teaches the performance abnormality detection condition includes a response

time from transmission of a response request message to the communication device to

reception of a response message corresponding to the response request message, and number

of times that the response time exceeds a predetermined threshold (Patrick: Column 25 Line 24

– 27 and Column 24 Line 10 – 12: an average response time exceeding a threshold value for a

DoS attack).

        It would have been obvious to a person of ordinary skill in the art at the time the

invention was made to combine the teaching of Patrick within the system of Kannon as modified

because (a) Kannon teaches detecting a denial of service attack on the server based upon the

performance level of load state of the data request / response traffic (Kannon: Abstract), and (b)

Patrick teaches providing a traffic monitoring unit for detecting a denial of service attack by

detecting an average response time exceeding a threshold value on a DoS attack (Patrick:

Column 25 Line 24 – 27 and Column 24 Line 10 – 12).

5.   Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kanno et al.

(U.S. Patent 2004/0064738), in view of Bang et al. (Korea KR-10-2004-0036228), and in view of

Costa et al. (U.S. Patent 2007/0006314).

As per claim 27, Kanno as modified does not disclose expressly each of the traffic

abnormality information and the performance abnormality information includes a certificate, and

the effects determining unit determines whether the communication device received the denial-

of-service attack, after performing an authorization based on certificates.

Costa teaches each of the traffic abnormality information and the performance

abnormality information includes a certificate, and the effects determining unit determines

whether the communication device received the denial-of-service attack, after performing an

authorization based on certificates (Costa: Para [0142]: verify the signature of a message using

the certificate to authenticate the message sending device in order to reduce the occurrence

and/or effect of denial of service attack to the network).

It would have been obvious to a person of ordinary skill in the art at the time the

invention was made to combine the teaching of Costa within the system of Kannon as modified

because (a) Kannon teaches detecting a denial of service attack on the server based upon the

performance level of load state of the data request / response traffic (Kannon: Abstract), and (b)

Costa teaches providing an improved method to reduce the occurrence and/or effect of denial of

service attack to the network by verifying the signature of a message using the certificate to

authenticate the message sending device (Costa: Para [0142]).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LONGBIT CHAI whose telephone number is (571)272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Longbit Chai/

Longbit Chai Ph.D.
Primary Patent Examiner
Art Unit 2431
10/07/2008